A survey on cybersecurity challenges and awareness for children of all ages

Siddiqui, Zeeshan; Zeeshan, Nida

Published in:
Proceedings 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE)

DOI:
10.1109/iCCECE49321.2020.9231229

Published: 23/10/2020

Document Version
Peer reviewed version

Siddiqui, D. Z., & Zeeshan, N. (2020). A survey on cybersecurity challenges and awareness for children of all ages. In M. H. Miraz, P. S. Excell, A. Ware, S. Soomro, & M. Ali (Eds.), *Proceedings 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE): Held Online as a Live Interactive Virtual Conference 17th-18th August, 2020* [9231229] IEEE. https://doi.org/10.1109/iCCECE49321.2020.9231229

A Survey on Cybersecurity Challenges and Awareness for Children of all Ages

Zeeshan Siddiqui[1] (Member, IEEE), Nida Zeeshan[2]

[1]*School of Computing, Engineering and Physical Science*
University of the West of Scotland, Scotland, UK
zeeshan.siddiqui@uws.ac.uk

[2]*School of Computer Science and Electronic Engineering*
University of Essex Colchester, UK
nidaciddiqui@gmail.com

***Abstract*—**Children are considered an easy prey to many cybersecurity threats. This is due to the lack of awareness of such threats while using smart devices, like smartphones. In most of the cases, not only children but their parents are also unaware of these security threats. Therefore, in this research, we have performed a comprehensive survey on various aspects of cybersecurity threats and its awareness among children. Such as, online safety and security for children, security control challenges and cybersecurity challenges for children and parents. We have also performed a security test to demonstrate the effectiveness of built-in security and privacy settings of such devices. For this purpose, we have used the built-in security and privacy settings of an iPhone 11 and performed various usage tests on unrestricted and restricted mode. The tests and observations have proved that the built-in security and privacy controls, such as Screen Time or Parental Controls, are the most effective way to safeguard children from various Cybersecurity threats they may face during their use of such devices and lack of cybersecurity awareness.

Keywords—information security, cyber security, security awareness, online safety, security and privacy, parental security controls.

I. Introduction

Children are considered most innocent, as well as most vulnerable to various aspects of threats. Let it be criminal activities, social activities or digital activities, children are considered an easy prey for criminal minds working anywhere. Thanks to the day-to-day advancements in our digital world, children are addicted to various smart devices and digital resources.

Other than the challenges related to children healthcare and well-being, children are considered more prone and vulnerable to the challenges and risks involved in the continuous and non-administered use of these technologies. There are various aspects of security challenges that can be linked with it. Such as, cybersecurity challenges and awareness among children, online safety and security while using mobile applications, games or contents, and the correct use of different security controls for parents. Therefore, in this study we have presented a survey on these security challenges while performing a security test by allowing children of various ages, to use a smartphone to play games and access web contents on restricted and unrestricted modes. The rest of the article is structured as follows. Section II has covered a detailed literature review followed by Section II, which is our security testing alongside survey and testing analysis on children behaviour while using the device in unrestricted and restricted mode. In Section IV, this study is concluded while weighing on the effectiveness of the correct and smart use of built-in security and privacy functions or settings of such devices to ensure children security and safety online.

II. Literature Review

In broader impact, cybersecurity threats are considered global challenge for every individual or a group. However, in order to achieve the objective of this study, the literature review is divided into various categories. Various safety and security challenges for children are discussed along with security control and awareness for children and parents/guardians.

A. Online safety and security for children

Authors of paper [1] have presented an ethnographic study on children while discussing privacy and security aspects. Various privacy rules and strategies are discussed in this study and several children perspectives are also brought forward. Various design implications are presented that covers children, households, and various security and privacy rules governing them.

In another paper [2], authors have discussed various risks and challenges about IoT and Smart homes. The study has discussed several ways to plan security in an IoT based environment by implementing and enforcing privacy rules, proper network segmentation and proper parental controls.

In another study [3] targeting security and privacy for kids through a project called *IoT4Kids*. Authors have presented their own customized checklist to alleviate the security and privacy risk for kids while discussing several methods carried out in this project. Based on these methods, authors have divided risks into several zones. These zones have covered, Authority, Discipline, Harms, Emotions, Governance and Accounting in a form of a checklist. Based on this checklist, authors are willing to extend their project into various steps based on feedback received from various involved entities.

A conceptual model for children safety on an internet environment is presented in another study [4]. The framework heavily depends on various techniques such as web-based analytics, sanitization of the data, mining of text, clustering and classification of the data appropriately. A conceptual model is utilized to deliver and control age-restricted information for children over an internet environment.

In another study [5], authors have conducted a survey based practical study targeting 12 children within the age range of 8-11. Based on this study it is recorded that children tends to solve risk and issues by themselves which they encounter, instead of taking them to their parents. It is also observed that children believe that the social media application owners or companies should invest more of their time and responsibility to provide much safer and secure online experience.

B. Security control challenges for children

Regarding rigorous security controls and measures, the authors have proposed and presented various techniques to automatically detect children presence using smart devices [6]. Techniques are based on children behaviour using smart devices to distinguish them from adults. Experiments to test the effectiveness and performance of those techniques is carried out with 99% accuracy and performance efficiency.

Similar control efficiency and child tracking system is presented in another study [7]. The proposed tracking system was based on the Android platform divided into two modules; one module is the parental control module, and another is the child module. Due to the sensitivity of the security at the child's end, the module consists of ARM7 chip, GPS, GSM, and voice controls inside the children module. Whereas, parent's module comprises of an Android-based dashboard for control and tracking.

Another study has discussed children addiction and online safety towards the use of smart devices [8]. The study is based on a mobile application delivering security awareness through storytelling. The application is divided into various levels of security awareness scenarios illustrated in a form of stories to engage students in a more influential way to gain security awareness through storytelling. The study is concluded while taking feedbacks and surveys from various students and teachers to address effectiveness of this study and possible future enhancements.

A patent level of study is presented to address security controls using server-based monitoring and control on various connected devices [9]. This unique control system has proposed various features, such as, learning gamification and numerous safety controls. It is highly compatible with other mobile applications and provide a unique feature to supersede internal control and access control based on game-based learning. It also features a remote access and control of remote client devices to provide and support better control and features.

In another study [10], a system and method has been proposed to identify objects being displayed in a media through a parental control mechanism. The proposed mechanism provides two levels of authentication to the children contents. First authentication level checks the second level of content authentication and provide a common authentication.

C. Cybersecurity awareness for children and parents

In another study to discuss cybersecurity awareness in school leaners in South Africa and the UK [11], various case studies are analyzed and supported by academia, industry and government. The study has analyzed various cybersecurity risks from individuals and groups to harm the learners intentionally. The study has also covered the existing scenario within these countries in academia, industry and government sectors. Study concluded with various recommendations based on key cybersecurity risks similarities and differences between the two countries.

In another contribution, a mobile game-based application was developed for cybersecurity awareness in children [12]. The game is developed specifically for K-6 age. The study has presented a conceptual framework based on a motivational model depending on Attention, Relevance, Confidence and Satisfaction. The evaluation is based on 12 Likert-type questions while successfully evaluating the effectiveness of the game for cybersecurity awareness.

In another study, a detailed survey is conducted on cybersecurity awareness, conceptual measures and practices [13]. The study is comprising of three stages. The first stage discusses the importance of cybersecurity awareness. Second stage discuss about various implementation of such awareness. Lastly, a conceptual framework is proposed to implement a better cybersecurity awareness.

In another study [14], a survey is conducted based on the collected data regarding the knowledge and teaching of Cyber Ethics, Cyber Safety and Cyber Security (C3). Various laws and professional standards are discussed based on C3 in K-12 schools. This study has also discussed various methods, instruments, awareness and instructional preparedness in teaching C3. The study is concluded while discussing various results and limitations in implementing teaching practice in C3.

In another study [15], various user characteristics are reported on various aspects. Such as, cybersecurity awareness levels, digital devices usage, and privacy issues. The result of the discussion is translated into various identities. As a result, four quadrants are generated while addressing various characteristics in Pro-active and Passive Multi-user and Pro-active and Passive Single user. The study is concluded with general finding and discussion on single user v/s multi-user and cybersecurity awareness level in different age group.

A chapter is written while discussing the promotion of cybersecurity compliance [16]. The chapter has discussed laws, standards and regulations to create and develop successful cybersecurity policies. This chapter has also discussed various tools to measure such compliance. Various theories of compliance are also discussed such as Deterrence

theory. The chapter is concluded with the various recommendation to maximize cybersecurity compliance.

A survey is conducted on the results of cybersecurity education on adults and other ages [17]. There are 233 participants in the survey. Majority of the result shows that there is a rise in concern about children usages of smart devices and lack of cybersecurity awareness. The survey has also asked whether the participants recommend awareness of cybersecurity through seminars.

III. Security Testing & Analysis

In the previous section, various studies are presented while discussing surveys and proposals to validate cybersecurity challenges and awareness in children. However, in almost all studies, no such security testing is carried out to examine different built-in security and privacy settings in a smartphone. Based on the literature review performed in the previous section, several studies have proposed various frameworks and proposals to recommend a better security and privacy platform for cybersecurity awareness for children. Many smart security and privacy frameworks and architectures are also proposed to tackle cybersecurity issues related to awareness [18]–[20]. However, it is to be noted that normal users, with limited or no cybersecurity awareness, are likely to be unaware of such enhancements and tools, and the ways to implement them.

Therefore, in this section, we have performed analysis based on built-in privacy and security settings within a Smartphone. For the purpose of this testing and analysis, we have used various privacy and security settings of an iPhone 11 and asked children of ages within 05 to 12 to use the phone. Children have been asked to play different iPhone games and browse different sites as normally they do. They were asked to do the following:

- Play games as per their age restrictions.
- Browse websites freely.
- Click anywhere or on any link of their choice.
- Perform any function they like to access offline or online contents.

Following pictures are going to demonstrate various customized privacy and security settings to test the behavior and activities of the children. To set up various security or parental environments. We have used the Screen Time privacy restrictions for iPhone 11, as depicted in Figures 1.0 and 2.0.

Figure 1.0 Screen Time

Figure 2.0 Content and Privacy

In the initial settings, we allowed all privacy options. Such as, Location Services, Contacts, Calendars, etc. We also allowed In-App purchases for iTunes and App store. However, we did restrict the phone to always ask for password as shown in Figures 3.0 and 4.0. In addition to this, we also put no restrictions in browsing websites by setting Web Contents to Unrestricted Access.

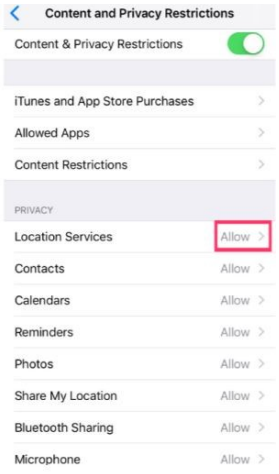

Figure 3.0 Privacy Settings

Figure 4.0 In-App Purchases

Additionally, children were also allowed to search contents online through web browser (Safari). They were also allowed to play multiplayer games and add friends in the game through social media accounts such as Facebook etc. Most importantly, they were allowed to change device passcodes, Apple account passwords and other related changes as depicted in Figures 05 and 06.

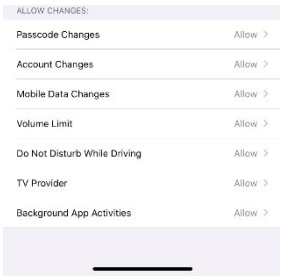

Figure 5.0 Allowed Changes

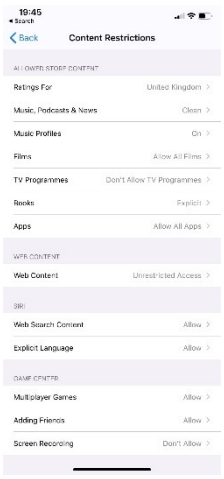

Figure 6.0 Multiplayer and Add Friends

Following Figures 7.0 and 8.0 depicts few of the mobile games installed for the children to play in both restricted and unrestricted settings. These games were chosen because of their support to multiplayer, social engineering application integration and in-app purchases features.

Figure 7.0 Disney Magic Kingdom

Figure 8.0 Cut the Rope

A. Behavioral Observations on Unrestricted Contents

Children from different ages were asked to use the phone continuously for several hours without any restrictions. Initially, children were asked to play installed games as single or multiuser. They were also asked to sign in using the provided Facebook credentials for them to play and invite others to join online.

They network was customized to act as a home/small network without any use of a Virtual Private Network (VPN) connectivity which is recommended for a more secure experience. Chosen games were all free games; therefore, children pressed several adverts and pop-up messages that lead them out of their games. Most of those adverts and pop-ups were not customized to suit the user interest. Many of the adverts and pop-ups opened external websites which were questionable according to their age and vulnerable to several security breaches. Many of the websites were not even using secure SSL channels. Children were heavily occupied in playing games, therefore, most of the children didn't try to read any adverts and pop-ups. Some of the pop-ups asked the children to allow the application or website to access device contents such as, Photos, Contacts, Emails etc. The primary motive of the children is to press any button to get rid of the pop-ups or messages and get back to their game which they were playing. Many of the children pressed the 'Yes' button instead of 'No' to unintentionally allow applications or websites to access the device contents.

During the user registration process in various games or websites, children were also asked to choose other type of identities rather than choosing an email address. Therefore, many of the children input mobile phone numbers as their identities to register. To make this more challenging, we associated a Credit Card with the Apple ID being used in the device as shown in Figure 9.0.

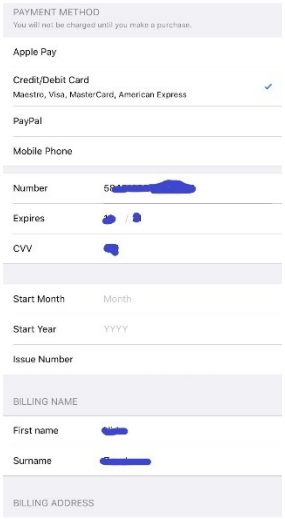

Figure 9.0. Apple Payment (Credit/Debit Card)

As all the games were free games, therefore, in-app purchases were required to buy items and unlock further game levels. Children proceeded with the in-app purchases and the applications or games took them to many external websites with a very basic security settings to process with the payments. Many of these websites even asked to store sensitive details with device credentials and payment information.

Many of these applications support chat functionality between game players or users. As the children were using social media credentials to play the games, therefore, majority of the team players in those games were just random unknown players.

Many of those unknown players or users sent SMS to the children using their registered mobile numbers which they have used to register their user. Some of them simply asked the children to share their payments details for them to unlock levels. Additionally, children also started to receive phishing

SMS with random links to click as shown in Figures 10 and 11.

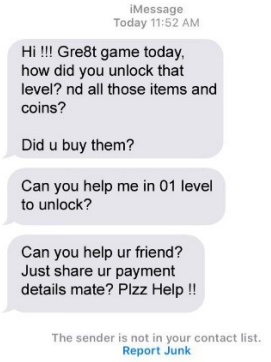

Figure 10 Random SMS asking about sensitive information

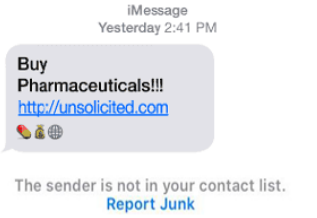

Figure 11 Phishing SMS

There were also few critical attempts to access and login to the Apple ID from different locations using a web browser and an iPhone as shown in Figure 12 and 13.

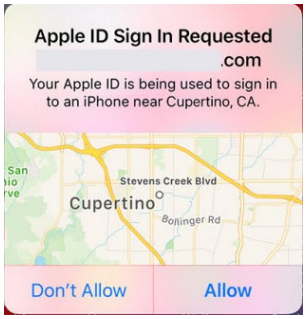

Figure 12 Login Attempt (Web)

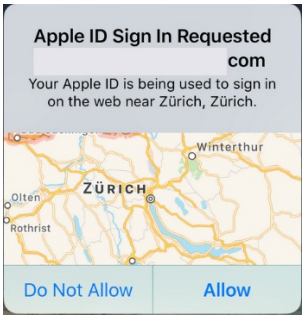

Figure 13 Login Attempt (iPhone)

B. Behavioral Observations on Restricted Contents

To observe children behaviour after imposing various restrictions, we restored the device to its original settings and put various restrictions as shown in the following Figures 14 and 15.

Children were only allowed to download and play games under the age range of 9-12. Web searching was not allowed with the restriction on the use of Explicit Language and Contents. Only few websites were allowed to be open like PBS Kids, CBeebies etc.

Children were also not allowed to play Multiplayer games. They were also not allowed to add friends or invite them to share games, contents and exchange chat messages.

The results and observations were overwhelming. Children were still receiving pop-ups and adverts; however, none were able to take them to any external sites where they can ask for further details. Children were also safely playing through their social media credentials, with the restriction to allow not to add friends or invite external or random players.

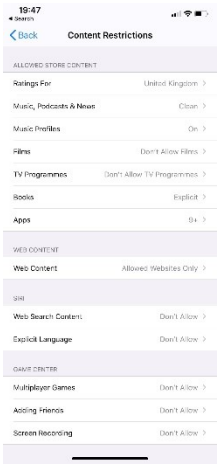

Figure 14 Content Restrictions

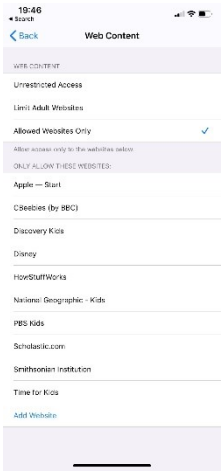

Figure 15 Allowed Websites Only

They didn't access any questionable or sensitive website due to the imposed restrictions. Also, as they didn't get the chance to invite other players online, therefore, they didn't get any suspicious SMS to ask for any sensitive information to share. There were no known attempts to login to the registered Apple ID associated with the device.

This testing and analysis have successfully proved the efficiency of built-in security and privacy settings of smart devices such as an iPhone 11. The smart use of such settings is vital for parents and carers to provide a controlled access to the devices being used by their children. Privacy controls and parental controls are handy when there is an absence or shortage of basic cybersecurity or information security awareness among children and/or parents.

IV. Conclusion

This study has presented a survey and a security analysis on the use of smart device, such as an iPhone, by Children of all ages. Children were given the opportunity to access mobile games and device contents while having unrestricted security and privacy settings. Later, children were allowed to use the device with a restricted built-in setting. Unrestricted mode has exposed children to wider cybersecurity threats, whereas, restricted mode gave them the opportunity to enjoy games and contents with caution and less chance of exposure to various security threats. This study has emphasized on the efficient and smart use of built-in security and privacy setting within a smartphone. As children are an easy prey to many Cybersecurity threats, therefore, it is highly recommended for the parents and carers to impose such settings to prevent children from various online security threats.

V. Acknowledgment

The work carried out in this article is supported by SICSA Cybersecurity Grant, SFC Project No: H07016.

REFERENCES

[1] J. A. Rode, "Digital parenting: designing children's safety," in *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, 2009, pp. 244–251.

[2] M. Sollars, "IoT security: could careless talk cost livelihoods?," *Comput. Fraud Secur.*, vol. 2019, no. 5, pp. 12–15, 2019.

[3] B. H. Knowles, S. Beck, G. Newmarch, J. Finney, and J. Devine, "IoT4Kids: Strategies for Mitigating Against Risks of IoT for Children," 2019.

[4] R. Alguliyev and S. Ojagverdieva, "Conceptual Model of National Intellectucal System for Children Safety in Internet Environment," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 3, p. 40, 2019.

[5] K. Badillo-Urquiola, D. Smriti, B. McNally, E. Golub, E. Bonsignore, and P. J. Wisniewski, "Stranger Danger!: Social Media App Features Co-designed with Children to Keep Them Safe Online," in *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, 2019, pp. 394–406.

[6] T. Nguyen, A. Roy, and N. Memon, "Kid on the phone! Toward automatic detection of children on mobile devices," *Comput. Secur.*, vol. 84, pp. 334–348, 2019.

[7] M. J. I. Susinthra and S. Praveena, "Children Tracking Classification Control Using Android," 2019.

[8] F. Lazarinis, K. Alexandri, C. Panagiotakopoulos, and V. S. Verykios, "Sensitizing young children on internet addiction and online safety risks through storytelling in a mobile application," *Educ. Inf. Technol.*, pp. 1–12, 2019.

[9] S. R. Schultz, "Learning gamification and safety control application for mobile devices." Google Patents, 14-Dec-2017.

[10] P. Sharma, "Systems and methods for presenting content simultaneously in different forms based on parental control settings." Google Patents, 13-Jun-2019.

[11] E. Kritzinger, M. Bada, and J. R. C. Nurse, "A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK," in *IFIP World Conference on Information Security Education*, 2017, pp. 110–120.

[12] F. Giannakas, G. Kambourakis, and S. Gritzalis, "CyberAware: A mobile game-based app for cybersecurity education and awareness," in *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, 2015, pp. 54–58.

[13] S. S. Tirumala, M. R. Valluri, and G. A. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," in *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 2019, pp. 1–6.

[14] P. Pusey and W. A. Sadera, "Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference," *J. Digit. Learn. Teach. Educ.*, vol. 28, no. 2, pp. 82–85, 2011.

[15] E. Kim, J. Yoon, J. Kwon, T. Liaw, and A. M. Agogino, "From Innocent Irene to Parental Patrick: Framing User Characteristics and Personas to Design for Cybersecurity," in *Proceedings of the Design Society: International Conference on Engineering Design*, 2019, vol. 1, no. 1, pp. 1773–1782.

[16] M. A. Harris and R. Martin, "Promoting cybersecurity compliance," in *Cybersecurity education for awareness and compliance*, IGI Global, 2019, pp. 54–71.

[17] J. Ricci, F. Breitinger, and I. Baggili, "Survey results on adults and cybersecurity education," *Educ. Inf. Technol.*, vol. 24, no. 1, pp. 231–249, 2019.

[18] N. Zeeshan, M. Reed, and Z. Siddiqui, "Three-way security framework for cloud based IoT network," in *International Conference on Computing, Electronics & Communications Engineering*, 2019, pp. 183–186.

[19] Z. Siddiqui, O. Tayan, and M. K. Khan, "Security analysis of smartphone and cloud computing authentication frameworks and protocols," *IEEE Access*, vol. 6, pp. 34527–34542, 2018.

[20] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart environment as a service: three factor cloud based user authentication for telecare medical information system," *J. Med. Syst.*, vol. 38, no. 1, p. 9997, 2014.